AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for masking digital data processed by a circuit executing an encryption algorithm comprising: ~~handled by an algorithm and factorized by a residue number system based on a finite base of numbers or polynomials prime to one another, comprising making the factorization base variable~~

calculating a plurality of factorizations of at least two input data based on a variable factorization base, the variable factorization base being comprised of elements prime to one another;

performing elementary operations on the plurality of factorizations to calculate a result factorization; and

combining the result factorization based on the variable factorization base to obtain a result.

2. (Currently Amended) The method of claim 1, wherein the elements of the variable factorization base ~~is~~ are chosen from a look-up table of sets of numbers or polynomials prime to one another.

3. (Currently Amended) The method of claim 2, wherein the ~~set of numbers or polynomials prime to one another used for the factorization by residue number system is~~ elements of the variable factorization base are randomly selected from the look-up table[[,]] for each new application of the algorithm.

4. (Currently Amended) The method of claim 1, wherein the elements of the factorization base ~~is~~ are calculated by a pseudo-random generator.

5. (Currently Amended) The method of claim 1, wherein the elements of the variable factorization base ~~is~~ are chosen to be compatible with the ~~lengths of the numbers or polynomials processed by the algorithm~~ input data.

6. (Currently Amended) The method of claim 1, ~~applied to input data already~~

~~factorized by a residue number system in an original base, the input data undergoing a factorization base change and the result provided by the algorithm undergoing, preferably, an inverse transformation towards said original base~~ wherein the at least two input data are at least two factorizations calculated based on a different factorization base, and wherein the result is a factorization in the different factorization base.

7. (Currently Amended) The method of claim 1, ~~applied to~~ wherein the at least two input data are not yet factorized.

8. (Currently Amended) The method of claim ~~1~~ 6, wherein ~~one or several factorization base changes are performed during the execution of the algorithm~~ the different factorization base is a variable factorization base .

9. (Currently Amended) A circuit comprising: ~~of algorithmic processing of data factorized by a residue number system based on a finite base of numbers or polynomials prime to one another, comprised of a circuit of selection or generation and of temporary storage of said base~~

a circuit to select a variable factorization base, the variable factorization base being comprised of elements prime to one another;

at least one circuit to calculate factorizations of input data based on the variable factorization base;

a circuit to perform elementary operations on the factorizations to calculate a result factorization;

a circuit to combine the result factorization based on the variable factorization base to obtain a result.

10. (Currently Amended) The circuit of claim 9, ~~comprising an element for storing a table of bases of numbers or polynomials prime to one another, said selection circuit selecting, at each application of the algorithm, a base from said table~~ wherein the circuit to select a variable factorization base comprises a memory to store a look-up table of sets of numbers or polynomials prime to one another from which the elements of the variable factorization base are

selected.

11. (Currently Amended) ~~the~~ The circuit of claim 9, ~~comprising an element for checking the conformity between the base selected for application of the factorizations by residue number system and the calculation circuits of the circuit executing the algorithm~~ further comprising a circuit for confirming that the variable factorization base is compatible with the input data.

12. (New) The method of claim 9, wherein the circuit to select a variable factorization base comprises a pseudo-random generator.

13. (New) The method of claim 1, wherein the at least two input data are at least two integers.

14. (New) A circuit comprising:

means for selecting a variable factorization base, the variable factorization base being comprised of elements prime to one another;

at least one circuit to calculate factorizations of input data based on the variable factorization base;

a circuit to perform elementary operations on the factorizations to calculate a result factorization; and

a circuit to combine the result factorization based on the variable factorization base to obtain a result.

15. (New) The circuit of claim 14, wherein the means for selecting comprises a means for storing a look-up table of sets of numbers or polynomials prime to one another from which the elements of the factorization base are selected.

16. (New) The circuit of claim 14, wherein the means for selecting comprises means for pseudo-randomly generating the elements of the variable factorization base.